6 ОСНОВНА ТЕОРЕМА АРИФМЕТИКИ

До дільників числа a завжди належать числа ± 1 і $\pm a$. Такі дільники числа a називаються *невласними*, а всі інші – *власними*. Зауважимо, що дільник b числа $a \neq 0$ буде власним тоді й лише тоді, коли він задовольняє нерівності $1 < |b| < |a|$.

Число, яке має власні дільники, називається *складеним*.

Натуральне число p, відмінне від 0 і 1, називається *простим*, якщо з того, що $p = xy$ для деяких цілих x, y, випливає, що x асоційований з p або y асоційований з p. При цьому, якщо x асоційований з p, то y асоційований з 1; якщо ж y асоційоване з p, то x асоційований з 1.

Альтернативне означення: натуральне число $p > 1$ називається *простим*, якщо у нього немає натуральних дільників, крім 1 і p.

Твердження 1 (властивості простих чисел) Нехай p – просте число. Мають місце наступні властивості:

1) якщо n – ціле число, і p ділить n, то p і n взаємно прості;

2) нехай $a, b \in \mathbb{Z}$; якщо p ділить ab, то p ділить a або p ділить b;

3) якщо p ділить добуток декількох цілих чисел, то p ділить хоча б одне з них;

4) довільне ціле число, більше 1, ділиться принаймні на одне просте;

5) простих чисел безліч;

6) якщо p_1 і p_2 – два різних простих числа, то вони взаємно прості.

Доведення.

1) Припустимо, що p не ділить n, і нехай $d = \gcd(n, p)$. При цьому $d \mid p$, тому d або асоційоване з p, або асоційоване з 1. Зауважимо, що d також ділить n, тому якщо d асоційоване з p, то p ділить n – протиріччя. Отже, d асоційоване з 1, звідки $n \perp p$.

2) Нехай p ділить ab, але не ділить a. За попередньою властивістю $a \perp p$, і по властивості взаємно простих чисел отримуємо, що $p \mid b$.

3) Індукція по n; база – пункт (2). $p \mid (a_1 a_2) a_3 ... a_n$, тому або $a_1 a_2$, або якесь з a_i (при $i > 2$) ділиться на p; якщо $a_1 a_2$ ділиться на p, то або a_1, або a_2 ділиться на p.

4) Нехай $n > 1$. Якщо n просте, доводити нічого. Якщо ж n не просте, то $n = n_1 m_1$ для деяких цілих чисел n_1, m_1, причому $1 < n_1 < n$ і $1 < m_1 < n$. Подивимося тепер на n_1: воно або просте, або ні; якщо воно не просте, можна знову записати $n_1 = n_2 m_2$, і так далі. Зауважимо, що $n > n_1 > n_2 > ....$, тому нескінченно довго цей процес тривати не може – всі ці числа натуральні. Отже, на якомусь етапі ми отримаємо просте число n_k; неважко бачити, що n на нього ділиться.

5) Припустимо протилежне; нехай $\{p_1, p_2, ..., p_k\}$ – множина всіх простих чисел. Розглянемо число $n = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$. За попередньою властивістю n ділиться на якесь просте число p; при цьому якщо $p = p_i$ для деякого i, то $1 = n - p_1 \cdot p_2 \cdot ... \cdot p_k$ ділиться на p_i, чого бути не може. Отже, число p не входить в множину $\{p_1, p_2, ..., p_k\}$.

6) Нехай p_1 і p_2 не взаємно прості; тоді за пунктом (1) маємо $p_1 \mid p_2$ і $p_2 \mid p_1$, тобто, вони рівні.

Теорема 1 (основна теорема арифметики) Кожне натуральне число може бути представлено у вигляді добутку простих чисел, і два таких розклади можуть відрізнятися тільки порядком запису співмножників.

Доведення.

Існування розкладу для натурального числа n доведемо індукцією по n. База: якщо $n = 1$, доводити нічого – добуток порожньої множини простих чисел дорівнює 1. Перехід: нехай тепер $n > 1$. За властивістю 4) простих чисел ми знаємо, що $n = p_1 n_1$ для деякого простого p_1. Тепер $n_1 < n$ і ми можемо застосувати припущення індукції до n_1: $n_1 = p_2 \cdot ... \cdot p_k$ для деяких простих $p_2, ..., p_k$. Звідси $n = p_1 p_2 \cdot ... \cdot p_k$ – добуток простих чисел.

Доведемо єдиність розкладу. Для цього знову проведемо індукцію по n. У разі $n = 1$ знову доводити нічого. Нехай $n = p_1 p_2 \cdot ... \cdot p_k = q_1 q_2 \cdot ... \cdot q_l$. Бачимо, що добуток $p_1 p_2 \cdot ... \cdot p_k$ ділиться на q_1. За властивістю 3) простих чисел один із співмножників $p_1, ..., p_k$ ділиться на q_1. Нехай це p_i: $q_1 \mid p_i$. Але за властивістю 6) простих чисел з цього випливає, що $p_i = q_1$. Поділимо тепер обидві частини рівності $p_1 p_2 \cdot ... \cdot p_k = q_1 q_2 \cdot ... \cdot q_l$ на $p_i = q_1$. Отриманий добуток менше n; за припущенням індукції, розклад в лівій і правій частинах відрізняються лише порядком проходження простих співмножників. Отже, і початкові розклади відрізняються лише порядком співмножників.

Нехай n – натуральне число. Згрупуємо однакові прості числа в розкладі n разом, розташуємо їх у порядку зростання і запишемо $n = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$, де $p_1 < ... < p_s$ – прості і $k_1, ..., k_s$ – натуральні числа. Такий (очевидно, однозначна) запис називається *канонічним розкладом* натурального числа n на прості множники.

Зауваження 1 Оскільки від'ємне число n можна записати у вигляді $n = -|n|$, то з основної теореми арифметики одразу випливає існування та однозначність розкладу в добуток простих множників і для від'ємних цілих чисел.

Зауваження 2 Тепер стає зрозумілим, чому число 1 не вважають простим: якби 1 відносили до простих чисел, то зникла б однозначність розкладу в добуток простих, бо до кожного розкладу можна було б приєднати довільну кількість множників 1.

Твердження 2 Нехай $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ – канонічний розклад числа n. Тоді кількість всіх натуральних дільників n дорівнює $(1+k_1)\cdot\ldots\cdot(1+k_s)$.

Твердження 3 Якщо $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, $n = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}$ для деяких простих $p_1 < p_2 < \ldots < p_s$:

$$d = \gcd(m, n) = p_1^{\min(k_1, l_1)} \cdot \ldots \cdot p_s^{\min(k_s, l_s)},$$

$$q = \operatorname{gcm}(m, n) = p_1^{\min(k_1, l_1)} \cdot \ldots \cdot p_s^{\min(k_s, l_s)}.$$

Приклад 1 Розкласти на прості множники число $3^{18} - 2^{18}$.

Розв'язання.

Користуючись формулами скороченого множення, отримуємо:

$$3^{18} - 2^{18} = \left(3^9 - 2^9\right)\left(3^9 + 2^9\right) = \left(3^3 - 2^3\right)\left(3^6 + 3^3 \cdot 2^3 + 2^6\right) \times$$

$$\times \left(3^3 + 2^3\right)\left(3^6 - 3^3 \cdot 2^3 + 2^6\right) = (3-2)\left(3^2 + 3 \cdot 2 + 2^2\right) \times$$

$$\times \left(3^6 + 3^3 \cdot 2^3 + 2^6\right)(3+2)\left(3^2 - 3 \cdot 2 + 2^2\right)\left(3^6 - 3^3 \cdot 2^3 + 2^6\right) =$$

$$= 1 \cdot 19 \cdot 1009 \cdot 5 \cdot 7 \cdot 577 = 5 \cdot 7 \cdot 19 \cdot 577 \cdot 1009.$$

Приклад 2 Побудувати канонічну форму чисел 12348 та 867, знайти кількість всіх їх натуральних дільників та їх НСД і НСК.

Розв'язання.

$12348 = 2^2 \cdot 3^2 \cdot 7^3$ – канонічне розкладання першого числа;

$867 = 3 \cdot 17^2$ – канонічне розкладання другого числа.

Дільників у першого числа буде $\tau = (2+1)(2+1)(3+1) = 36$, а у другого $\tau = (1+1)(2+1) = 6$.

$$\text{НСД} - d = \gcd(12348, 867) = 2^{\min(2,0)} \cdot 3^{\min(2,1)} \cdot 7^{\min(3,0)} \cdot 17^{\min(0,2)} = 3;$$

$$\text{НСК} - q = \operatorname{gcm}(12348, 867) = 2^{\max(2,0)} \cdot 3^{\max(2,1)} \cdot 7^{\max(3,0)} \cdot 17^{\max(0,2)} = 4235364.$$

Приклад 3 Знайти всі такі натуральні прості числа p, для яких кожне з чисел $p+4$ і $p+14$ також буде простим.

Розв'язання.

Розглянемо остачі від ділення цих чисел на 3. Із рівностей $p+4 = 3+(p+1)$ і $p+14 = 12+(p+2)$ випливає, що числа p, $p+4$ і $p+14$ при діленні на 3 дають різні остачі. Отже, одна з цих остач дорівнює 0, тобто одне з цих чисел ділиться на 3. Але числа $p+4$ і $p+14$ прості й більші, ніж 3, тому вони на 3 не діляться. Звідси $3 \mid p$ і $p = 3$, бо p – просте. Оскільки числа $3+4 = 7$ і $3+14 = 17$ – прості, то $p = 3$ справді задовольняє умову задачі.

Приклад 4 Якою буде відповідь у попередньому прикладі, якщо не вимагати, щоб число p було натуральним?

Розв'язання.

Як і в попередньому прикладі, доводимо, що одне з простих чисел p, $p+4$ і $p+14$ ділиться на 3. Це дає нам 6 випадків: 1) $p=3$; 2) $p=-3$; 3) $p+4=3$; 4) $p+4=-3$; 5) $p+14=3$; 6) $p+14=-3$. Перевірка показує, що у 2-му і 3-му випадках не будуть простими відповідно числа $p+4$ і p, а в решті випадків всі числа p, $p+4$ і $p+14$ будуть простими.

Це дає 4 розв'язки: $p=3$, $p=-7$, $p=-11$, $p=-17$.

Приклад 5 Довести, що існує нескінченно багато простих чисел вигляду $4k+3$.

Розв'язання.

Зауважимо, що кожне непарне число має вигляд $4k+1$ або $4k+3$, і що добуток чисел вигляду $4k+1$ знову буде числом такого ж вигляду: $(4m+1)(4n+1)=4(4mn+m+n)+1$. Тому не може бути, щоб у розкладі числа вигляду $4k+3$ у добуток простих всі множники були вигляду $4k+1$. Отже, кожне число вигляду $4k+3$ має хоча б один простий дільник такого ж вигляду. Далі, припустимо, що простих чисел вигляду $4k+3$ – скінченна кількість, і нехай $p_1, ..., p_k$ – їх повний список. Число $n=4p_1...p_k-1=4\cdot(p_1...p_k-1)+3$ є числом вигляду $4k+3$ і не ділиться на жодне з чисел $p_1, ..., p_k$. Тому той простий дільник числа n, який має вигляд $4k+3$, не зустрічається у списку $p_1, ..., p_k$. Отже, припущення про скінченність простих чисел вигляду $4k+3$ приводить до протиріччя.

У багатьох книгах з теорії чисел наводяться таблиці натуральних простих чисел, що не перевищують даного числа N. Простий метод побудови таких таблиць запропонував близько 200 р. до н.е. грецький математик з Александрії Ератосфен. Цей метод, відомий під назвою *решета Ератосфена*, виглядає так:

а) обираємо перше просте число $p_1=2$;

б) викреслюємо всі цілі числа з інтервалу $(2, N)$, кратні 2;

в) обираємо наступне найменше просте число $p_2=3$;

г) викреслюємо всі цілі числа з інтервалу $(3, N)$, кратні 3;

ґ) повторюємо процес із наступним $p_3=5$;

д) обираючи чергове p_k, звертаємо увагу на те, що кандидатів на викреслення необхідно розглядати з p_k^2, оскільки до цього числа всі складені викреслені, як такі, що кратні простим числам, меншим за p_k;

е) викреслення можна зупинити, коли p_k перевищить N. Усі кратні числа на той час будуть викреслені.

Приклад 6 Відомо, що всі дільники числа n, відмінні від 1, більші, ніж $\sqrt{n}$. Доведіть, що число n просте.

Розв'язання.

Нехай число n складене. Тоді $n=k_1\cdot k_2$, де $k_1>1$ і $k_2>1$. За умовою $k_1>\sqrt{n}$ і $k_2>\sqrt{n}$. Звідси $k_1\cdot k_2>n$. Отримали суперечність.

Зауваження. Враховуючи приклад 1.42, при побудові решета Ератосфена досить викреслювати кратні лише тих простих чисел, які не перевищують $\sqrt{N}$. Це значно зменшує об'єм обчислень.

Приклад 7 За допомогою решета Ератосфена знайти всі прості числа з проміжку $[1230, 1250]$.

Розв'язання.

Оскільки $\sqrt{1250} < 36$, то з проміжку $[1230, 1250]$ досить викреслити кратні лише тих простих чисел, що не перевищують 35, тобто кратні числам 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 і 31 . Після викреслювання чисел, кратних 2, 3 і 5, не викресленими залишаться тільки числа 1231, 1237, 1241, 1243, 1247 і 1249. Остачі від ділення 1230 на прості числа 7, 11, 13, 17, 19, 23, 29 і 31 дорівнюють відповідно 5, 9, 8, 6, 14, 11, 12 і 21. Тому на проміжку $[1230, 1250]$ кратними цих простих чисел будуть:

число p	його кратні	число p	його кратні
7	1232, 1239, 1246	19	1235
11	1232, 1243	23	1242
13	1235, 1248	29	1247
17	1241	31	1240

Якщо викреслити й ці кратні, то не викресленими залишаться числа 1231, 1237 і 1249. Вони і є шуканими.

Приклад 8 Спираючись на основну теорему арифметики, довести ірраціональність числа $\sqrt{2}$.

Розв'язання.

Припустимо, що $\sqrt{2}$ – раціональне число. Тоді його можна записати у вигляді дробу $\sqrt{2} = \frac{a}{b}$. Після піднесення обох частин рівності до квадрату одержимо: $2b^2 = a^2$. Але в канонічному розкладі числа $2b^2$ число 2 зустрічається з непарним показником, а в канонічному розкладі числа a^2 – з парним. Отже, припущення про раціональність числа $\sqrt{2}$, що приводить до протиріччя з однозначністю канонічного розкладу.

Теорема 2 (мала теорема Ферма) Якщо натуральне число a не ділиться націло на просте число p, то $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Доведення.

Розглянемо $p-1$ число: a, $2a$, $3a$, …, $(p-1)a$. Очевидно, що кожне із цих чисел не ділиться націло на p. Нехай r_1, r_2, …, r_{p-1} – їхні остачі при діленні на p відповідно. Доведемо, що жодні два з розглядуваних чисел не дають однакових остач при діленні на p.

Припустимо, що такі два числа знайдуться. Позначимо їх ma і na, де $1 \le m \le p-1,\ 1 \le n \le p-1,\ m > n$. Тоді $(ma - na) \vdots p$, тобто $(m-n)a \vdots p$. Проте, НСД$(a;\ p) = 1$. Тоді $(m-n) \vdots p$, що неможливо, оскільки $0 < m-n < p$.

Оскільки при діленні на число p існує $p-1$ ненульова остача, а числа a, $2a$, $3a$, …, $(p-1)a$ дають різні остачі при діленні на p, то отримуємо:

$$\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}.$$

Маємо:

$$a \equiv r_1 \pmod p \equiv 1 \pmod p,$$
$$2a \equiv r_2 \pmod p \equiv 2 \pmod p,$$
$$\ldots,$$
$$(p-1)a \equiv r_{p-1} \pmod p \equiv p-1 \pmod p.$$

Звідси $a \cdot 2a \cdot ... \cdot (p-1)a \equiv r_1 \cdot r_2 \cdot ... \cdot r_{p-1} \pmod p \equiv 1 \cdot 2 \cdot ... \cdot (p-1) \pmod p$ або $a^{p-1} \equiv 1 \pmod p$.

Наслідок. Для будь-якого числа a і простого числа p маємо: $a^p \equiv a \pmod p$.

Приклад 9 Знайти всі такі натуральні числа n, що числа $n+1$, $n+11$, $n+27$ є простими.

Розв'язання.

Оскільки різниця жодних із двох даних чисел не ділиться націло на 3, то всі вони дають різні остачі при діленні на 3. Отже, одне із цих чисел кратне 3, а оскільки воно є простим, то саме воно дорівнює 3. Очевидно, що це може бути тільки число $n+1$, звідки $n=2$. Тоді $n+11=13$, $n+27=29$.

Відповідь: $n=2$.

Приклад 10 Розв'яжіть у простих числах рівняння $x^y + 1 = z$.

Розв'язання.

Якщо $x \ne 2$, то x – непарне число, і ліва частина рівняння більша за 2 та є парним число. У цьому випадку число z простим бути не може.

Отже, $x=2$. Маємо: $2^y + 1 = z$. Якщо y – непарне число, то число $2^y + 1$ можна розкласти на множники, кожний з яких більший за й. знов-таки у цьому випадку число z простим бути не може. Звідси y – парне просте число, тобто $y=2$. Тоді $z = 2^2 + 1 = 5$.

Відповідь: $x=2,\ y=2,\ z=5$.

Приклад 11 Знайдіть остачу від ділення числа 3^{102} на 101.

Розв'язання.

Оскільки 101 – просте число, то за малою теоремою Ферма

$$3^{100} \equiv 1 \pmod{101}.$$

Звідси, $3^{102} \equiv 9 \pmod{101}$.

Відповідь: 9.

Приклад 12 Доведіть, що коли натуральне число n не ділиться націло на 17, то або $\left(n^8-1\right)\vdots 17$, або $\left(n^8+1\right)\vdots 17$.

Розв'язання.

За малою теоремою Ферма

$$n^{16}\equiv 1\left(\mathrm{mod}\,17\right),$$

звідки $\left(n^{16}-1\right)\vdots 17$, $\left(n^8-1\right)\left(n^8+1\right)\vdots 17$. Отже, або $\left(n^8-1\right)\vdots 17$, або $\left(n^8+1\right)\vdots 17$.